



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
PO Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/883,371	06/19/2001	Shuji Shichi	PNDF-01078	1070
466	7590	05/29/2008	EXAMINER	
YOUNG & THOMPSON			DASS, HARISH T	
209 Madison Street			ART UNIT	PAPER NUMBER
Suite 500			3692	
ALEXANDRIA, VA 22314			MAIL DATE	DELIVERY MODE
			05/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/883,371

Filing Date: June 19, 2001

Appellant(s): SHICHI, SHUJI

Roland E. Long, Jr. (Reg. 41,949)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 4/7/2008 appealing from the Office action mailed 7/19/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner. Claim Rejections under 35USC §112 first paragraph and also second paragraph of claims 16-29 (see paper number 20071108).

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

US 2003/0200179	Kwan	10-2003
US 5,239,583	Parrillo	8-1993
US 6,701,522	Rubin et al.	3-2004
US 6,636,973	Novoa et al.	10-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

DETAILED ACTION

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 16-21 and 30-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kwan (US 2003/0200179) in view of Parrillo (US 5,239,583).

Re. Claim 16, Kwan discloses prepaid card and a method for making payment to merchant through electronic network to settle a transaction [Abstract; Figures 2-3],

A) providing a user with a prepaid card linked to a database [Figure 5; paragraphs (para.) 04, 06 "is instantaneous and there is no waiting period like ... is already pre-paid."

Mean settled; para. 20]; and

B) executing a first action chain forⁱ immediately settling a data sale including sequentially [Figures 2-3; para. 06 "There are many ... users to make payment ... already pre-paid"; para. 61 "at step 270, the ... the amount is accepted" and "Thank you for your payment "Merchant" of 50 dollars ... You have 40 dollars balance ... pre-paid card" means settling the sale/payment].

i) the user inputting a password number [para. 21; 32-33],

ii) a first validation of the prepaid card by comparing the user-input password number to a system-set first-time password number stored on the database as the current password number [Figures 3-5; claim 5 (see verifying the password identification code, new users to select a unique password); para. 21, para. 60-61 see "It will check to see if the customer's payment code (payment code or pre-paid card password). It is obvious that there is a first time password either set by system administrator or customer/merchant, where in case of administrator's set-password, it is encouraged to be changed 1

iv) requesting a current monetary balance available on the prepaid card [claim 5; para. 32-33 (inputting queries)]

C) executing another action chain including sequentially and wherein step C) is repeated [see Abstract "This is a pre-paid card system to store monetary value and subsequently for making payment to merchants": Figures 2-3: see Figure 3 for

sequence of steps including "You have 40 dollars balance" which can be used for another transaction – repeating is inherently in Kwan (making payments to other merchants using the same card)],

Kwan does not explicitly disclose

- iii) the user entering a next-time password number and storing the user-input next-time password number in the database as a new user-set password number,
- ii) validation of the prepaid card by a successful comparison of the user-input another password number to the stored new, user-set next-time password,
- iii) the user entering another next-time password number and storing the user-input another next-time password in the database as the new, user-set next-time password number required for validation of the prepaid card in a next another action chain.

However, inputting or entering password, validation of passwords and changing the passwords are well known to protect unauthorized use of computer accounts, credit cards, and debit cards. For example (well-known), a bank customer who has opened an account with a bank receives a debit card (credit card, IC card, or smart card) by mail and a temporary password or PIN (separately mailed by the bank), customer activates the card (using ATM, PC or phone)¹ and changes the PIN (initial password or first time password) to new PIN (password) and now the new PIN is activated and can be used for next transaction. It is known that validation of password (current password, next-time password, etc) is comparing the inputted password with record of password associated

with user id in database, and changing password mean changing the record of password in the database using SQL. Example 2; a bank account customer making a payment using Internet, 1) customer using bank's URL/portal opens the bank web page, 2) from site menu selects service and logs to online banking by entering user id and password, 3) selects his account and bill payment menu and makes payment 4) before/after making payments (step 3) customer has an option to change his/her password if or she wants, 5) logs off, 6) for next time login, he/she has to use new password, 7) these sequence of steps 1-6 can be repeated for next bill payment. Further, customer is free to change his/her PIN any time he/she wants before transaction/checking emails or after it is personal preference or business choice, a very careful person may change it every 15 days or a month and a paranoid person may change it every other usage. At USPTO user password must be change within 3 months, dynamic RSA SecurID token changes the password continuously, every minute which means user logs-in with current password which is different than a password a minute before it and it will be different from a password the next minute. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the disclosure of Kwan and include provisioning for changing password as often as use wishes and at any time before a bill payment/checking email or after it to increase the security of the password protection.

Parrillo discloses iii) the user entering a next-time password number and storing the user-input next-time password number in the database as a new user-set password

¹ Comparing the pin/password with database for authentication/validation and storing of the new

number, ii) validation of the prepaid card by a successful comparison of the user-input another password number to the stored new, user-set next-time password, iii) the user entering another next-time password number and storing the user-input another next-time password in the database as the new, user-set next-time password number required for validation of the prepaid card in a next another action chain [Abstract; col. 2 lines 10-46; col. 3 line 58 to col. 4 line 25 also col. 6 lines 26-50 and claim 1]. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the disclosure of Kwan and include the above steps to allow the users to change password as often as he/she wishes at any time including for next transaction, as it is disclosed by Parrillo, to prevent usage of card by unauthorized user observing a successful transaction where the subsequent duplication of that exact same access code would result in failure to access the account and enhance the security of the pre-paid card usage.

Re. Claim 17, Kwan discloses wherein the prepaid card is a virtual card [para 09; 05; 18].

Re. Claim 18, Kwan discloses the prepaid card comprises a physical card carrying duplicate information carried in the database, the prepaid card comprises a serial number, the first-time password number, and an expiration date printed on an exterior surface of the physical card, and the database comprises the serial number, the first-

time password number, and the expiration date of the prepaid card [Figure 1; para 21; 63; claim 1]

Re. Claim 19, Kwan discloses the first-time password number is concealed below of scratch-off covering [Figure 5; para 21].

Re. Claim 20 Kwan discloses the database includes a database record corresponding to the prepaid card and comprising a serial number field storing a system-assigned serial number, a first-time password number field storing the system-assigned first-time password number used for a first time validation of the prepaid card, and a user-set password number field for storing the user-set next-time password number (password) reset by the user subsequent to each validation of the prepaid card, a monetary balance field storing a monetary balance available to the user [Figures 2-3; para. 19-21; claim 8;], and comprising the further step of: subsequent to the validation of the prepaid card, a action of subtracting a price being necessary for distribution from monetary balance field to update the monetary balance field by reducing a value of the monetary balance field by the price being subtracted [para 21; 32-35; claim 5].

Re. Claim 21 Kwan discloses an issue date field, an expiration date field, a card monetary face value field, a transaction product/service number field , and a transaction date field, each having a one-to-one correspondence with the prepaid card [Figures 4-5; para 75; 93; 69].

Re. Claim 30, claim 30 is rejected with same rational as claim 16.

Re. Claim 31, Kwan discloses the card comprises a physical card carrying duplicate information carried in the database [Figure 1; para. 21; 63; claim 1], and the card each comprises a serial number, the first-time password number, and an expiration date printed on an exterior surface of the physical card [Figure 1; para 21; 63; claims 1 & 4].

Re. Claim 32, Kwan discloses the database includes a database record corresponding to the card and comprising a serial number field storing a system-assigned serial number, a first-time password field storing the system-assigned first-time password used for a first time validation of the card, and a user-set password field for storing the user-set password reset as the current password number by the user subsequent to each validation of the card, a monetary balance field storing a monetary balance available to the user, and comprising the further step of: subsequent to the validation of the card, a action of subtracting a transaction' price for distribution to a vendor from the monetary balance field to update the monetary balance field by reducing a value of the monetary balance field by the price being subtracted [Figures 2-3; para. 19-21; 32-35; claims 5 & 8].

Re. Claim 33 Kwan discloses an issue date field, an expiration date field, a card monetary face value field, a transaction product/service number field, and a transaction date field, each having a one-to-one correspondence with the card [Figures 4-5; para. 75; 93; 69].

Claim 22-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kwan and Parrillo as it applied to claims 16 and 20 above, and further in view of Rubin et al (hereinafter Rubin – US 6,701,522).

Re. Claims 22-24, Kwan discloses located between a user and the database, receiving from the user an input of the card serial number and the user input another password (password) number; the portal accessing the database and validating the prepaid card by comparing the received user-input another password (password) number with the next-time password (password) number stored on the database [claim 1], and wherein the portal site is connected to the user and to the database via the Internet and wherein the portal site is connected to the user via a telephone line and (see use of internet and telephone for activation) [para. 60; claim 1]. Kwan or Parrillo does not explicitly disclose portal, or a portal site. However, Rubin discloses this feature [see Abstract; Figures 1-2, 7; col. 1 lines 5-50] to allow a user(s) (purchaser) to customize interested websites, which will be automatically retrieved and display information the user is seeking. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the disclosure of Kwan, Parrillo and include portal, as disclosed by Rubin, to allow the user to configure its favorite's website for obtaining information or purchases.

Re. Claim 25, Kwan discloses wherein the user orally inputs another password (password) number to the portal [para. 60].

Re. Claim 26, Rubin discloses portal site. Kwan, Parrillo or Rubin does not explicitly disclose further receives user input of the serial number and confirms the expiration date of the prepaid card to the database prior to validating the prepaid card. However, this function is well known function of using credit cards. For example, when a customer orders a product online or by phone the merchant asks these questions to properly charge the customer as-will-as validates the card. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the disclosure of Kwan, Parrillo and Rubin and include this function to enhance the security of the card in case it is used improperly.

Re. Claim 29, Kwan discloses wherein the user orally inputs the password number to the portal site and the portal site orally responds to the user, via a telephone call [para. 60].

Claim 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kwan, Parrillo and Rubin as it applied to claims 16, 20 & 26 above, and further in view of Novoa.

Re. Claims 27-28, Novoa discloses after validation of the prepaid card, the portal site i) requests the user to input the new user-set next-time password (password) number, ii) receives the new user-set password number from the user, iii) sends the received new user-set next-time password (password) number to the database to be stored, in the

user-set next-time password/password number field, as the text-time password/password number required for a next validation of the prepaid card and a next successful validation of the prepaid card requires the portal site i) to receive from the user another password number input, 'and ii) to successfully compare the received another password number input with the next-time password/ password number stored in the user-set password number field of the record of the prepaid card within the database [Abstract; col. 2 lines 27-49; col. 3 lines 6-25] to increase the security for unauthorized access to the account since the current pre-paid card have code printed on them and any one can use it if the card is lost or stolen. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the disclosures of Kwan, Parrillo and Rubin and include provisioning for the user to reset password, as disclosed by Novoa, for enhancing the security of the pre-paid card and storing the new password in database for validation of the card to prevent fraud and misuse of the customer pre-paid account.

Claims 34-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kwan and Parrillo as applied to claims 30 & 32 above, and further in view of Novoa et al. (hereinafter Novoa –US 6,636,973) and Rubin.

Re. Claims 34-35, Novoa discloses a server, located between a user and the database, receiving from the user an input of the card serial number and the currently user input password; the portal accessing the database and validating the card by comparing the

received user-input password with the current password stored on the database, and after validation of the card, the portal site i) requests the user to input the new user-set password, ii) receives the new user-set password from the user, iii) sends the received new user-set password to the database to be stored, in the user-set password field, as the current password required for a next validation of the card [Abstract; col. 2 lines 27-49; col. 3 lines 6-25] to increase the security for unauthorized access to the account since the current pre-paid card have code printed on them and any one can use it if the card is lost or stolen. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the disclosures of Kwan and Parrillo and include the above steps and provisioning for the user to reset password, as disclosed by Novoa, for enhancing the security of the pre-paid card and storing the new password in database for validation of the card to prevent fraud and misuse of the customer pre-paid account. Rubin discloses portal, or a portal site [see Abstract; Figures 1-2, 7; col. 1 lines 5-50]. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the disclosure of Kwan, Parrillo and Novoa and include portal, as disclosed by Rubin, to allow the user to configure its favorite's website for obtaining information or purchases.

(10) Response to Argument

In response to applicant's argument recitation page 7 "The Examiner bears the initial burden of presenting a *prima facie* case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992). ..." A mere statement or argument that the Office has not established a *prima facie* case of obviousness or that the Office's reliance on common

knowledge is unsupported by documentary evidence will not be considered substantially adequate to rebut the rejection or an effective traverse of the rejection under 37 CFR 1.111(b) (See *In re KSR*).

During patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification." >The Federal Circuit's en banc decision in *Phillips v. AWH Corp.*, 415 F.3d 1303, 75 USPQ2d 1321 (Fed. Cir. 2005) expressly recognized that the USPTO employs the "broadest reasonable interpretation" standard:

The history of prosecution is the evidence that the Examiner has fulfilled his duty and has provided office rejections, according to MPEP, which indicates that the invention is not patentable distinguished from prior arts and it is an obvious *prima facie* since the claimed invention is merely a combination of old elements, and in the combination each element merely would perform the same function as it did separately, and one of ordinary skill in the art would recognized that the results of the combination were predictable (see paper number 20070716).

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., In response to applicant's argument recitation page 7 "As discussed above, the present invention provides a user-supplied "next-time" password as part of each card validation and set by the user prior to accessing the card's monetary balance. A user-set password is a password set by the user and not a password set by the system.") are not recited in the rejected claim(s). Although the claims are interpreted in light of the

specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., In response to applicant's argument recitation page 7 "user entering another password ... The claims are not directed to merely replacing the password with each use of the prepaid card") are not recited in the rejected claim(s). The claimed invention has been given a broadest reasonable interpretation and has established a *prima facie* case of obviousness (See Supra.)

In response to applicant's argument that "KWAN teaches that the next-time password set by the ..." KWAN is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Kwan is analogous art for settling a transaction using prepaid card where prepaid card has a security feature (at least see Kwan para. 21 "security number imbedded under some scratch-off material") and card validation (claim 5) and inputting a password (claim 5; paragraph 13).

In response to applicant's argument (page 8) that "On pages 5-6 of the Official Action, there is a paragraph that lists "well known" actions. That these are well known now (i.e., in July 2007 when the Official Action was mailed) is not evidence that these

actions were known to one skilled in the art at the time of the invention. It is clear error to rely on facts not supported by the record. A rejection including such clear error is improper." 1) "well-known" means they were known (obvious and commonly known to one ordinary skill in the art) at the time of invention. Applicant with knowledge of technology has not provided any documentary evidence that the Examiner has made an error and these elements were unknown at the time of invention and are Applicant's invention. Even, reviewing, at least, the submitted prior art of record will show (explicitly or implicitly) that these are old and well-known elements.

In response to applicant's argument (page 9) that "Examiner offers PARRILLO as teaching the user entering a next- time password as a new, user-set next-time password number. This is a factual error as the PARRILLO password is not a user-set password as required by the claim. ..." 1) the office action clearly has stated as of limitations disclosed by secondary reference Parrillo (see Col.) Parrillo (Abstract; Col. 2 lines 10-46; Col. 3 line 58 through Col. 4 line 25; Col. 6 lines 26-50 and claim 1) and the rational of combining the secondary reference (Parrillo) with other elements are stated in office action, see paper number 20070716 pages 6-7.

2) Parrillo is an analogous art "Known Work in One Field of Endeavor May Prompt Variation of it for Use in Either the Same Field or a Different One Based on Design Incentives or Other Market Forces if The Variations Would Have Been Predicable to One of Ordinary Skill in the Art." See In re KSR.

In conclusion, the claimed invention is not distinguished from prior art of record. The claimed invention is merely a combination of old elements, and in the combination

each element merely would perform the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Harish T Dass/
Primary Examiner, Art Unit 3692

Conferees:

Kambiz Abdi /K. A./

Supervisory Patent Examiner, Art Unit 3692

Vincent Millin /V/M/
Appeals Practice Specialist

¹ "For" - intended used.